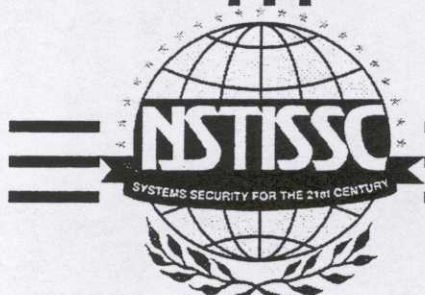


UNCLASSIFIED

NSTISSAM INFOSEC/1-00
8 February 2000



**ADVISORY MEMORANDUM
FOR THE USE OF THE
FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) 140-1
VALIDATED CRYPTOGRAPHIC MODULES IN PROTECTING
UNCLASSIFIED NATIONAL SECURITY SYSTEMS**

**THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER
IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.**

UNCLASSIFIED

UNCLASSIFIED



National Security Telecommunications and Information Systems Security Committee

NATIONAL MANAGER

FOREWORD

1. This Advisory Memorandum provides guidance to U.S. Government departments and agencies regarding the application of Federal Information Processing Standard (FIPS) 140-1 to the validation of cryptographic modules which may be used to protect UNCLASSIFIED information within computer and telecommunications systems that are not national security systems. As noted, responsibility for establishing security standards for national security systems remains the responsibility of the Director of the National Security Agency.

2. Issuance of the document represents another step in a continuing effort to keep departments and agencies apprised of significant information systems security or information assurance developments which may impact on the operations and activities of their respective organizations. Consistent with the existing working partnership, the National Security Agency (NSA) has coordinated this document with the National Institute of Standards and Technology (NIST).

A handwritten signature in dark ink, reading 'Michael V. Hayden'.

MICHAEL V. HAYDEN
Lieutenant General, USAF

UNCLASSIFIED

**ADVISORY MEMORANDUM
FOR THE USE OF
FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) 140-1
VALIDATED CRYPTOGRAPHIC MODULES IN
PROTECTING UNCLASSIFIED NATIONAL SECURITY SYSTEMS**

SECTION I - GENERAL BACKGROUND

1. FIPS 140-1 specifies the security requirements to be satisfied by a cryptographic module utilized within computer and telecommunication systems protecting unclassified information. The security requirements cover areas related to the secure design and implementation of a cryptographic module to include basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference/electromagnetic compatibility (EMI/EMC), and self-testing.

SECTION II - APPLICABILITY AND LIMITATIONS

2. FIPS 140-1 has been made mandatory and binding by the Secretary of Commerce

4. It must be emphasized that the FIPS 140-1 standard specifies only the security requirements for cryptographic modules. The standard does not specify product or system level security requirements, nor does it specify cryptographic interoperability. Similarly, the NIST FIPS 140-1 CMV Program validates cryptographic modules. This process and associated certificates should not be viewed as a validation of the non-cryptographic security functionalities of a security or security-enabled information technology product. Often, the security functionalities in such products, such as access control and authentication, are achieved by non-cryptographic mechanisms such as passwords and biometrics. ~~It should be understood that~~ vendor claims or advertisements claiming FIPS 140-1 compliance, apply only to the cryptographic modules or modules incorporated into the product, not to the product in its entirety. The scope of validation is contained on the validation certificate. Nevertheless, the FIPS 140-1 CMV Program provides significant value in the validation of the cryptographic module contained in the security product. In many cases, this cryptographic module is a critical component of the overall security functionality provided by the product.

SECTION III - USE OF FIPS 140-1 VALIDATED CRYPTOMODULES IN UNCLASSIFIED "NATIONAL SECURITY SYSTEMS"

5. National security systems (as defined in USC 40, Section 1452) are not subject to FIPS 140-1. Nevertheless, DoD customers often request guidance from NSA regarding the advisability of using commercial products (e.g., PGP) which contain FIPS 140-1 approved modules to protect unclassified information in national security systems.

6. While NSA recommends the acquisition of security products which have been evaluated to determine the robustness of their complete security functionality (preferably against NSA or NIST sponsored Common Criteria (CC) Protection Profiles), products which contain FIPS 140-1 validated encryption modules may be used for the cryptographic protection of unclassified information in national security systems. NSA and NIST produced product level CC protection profiles targeted at unclassified environments will require FIPS 140-1 validated or NSA endorsed cryptographic modules when cryptographic security functional requirements exist in the product.

SECTION IV - FIPS 140-1 APPROVED ALGORITHMS

7. FIPS 140-1 contains language which requires the use of FIPS-approved cryptographic algorithms. For the purposes of providing data confidentiality for unclassified information, the NIST-approved algorithms are the Data Encryption Standard (DES), Triple DES and SKIPJACK.

8. For the purposes of protecting unclassified information in national security systems, however, NSA has determined that the DES algorithm is inadequate. For more information on

SECTION V - CAUTION AND CONCLUSION

9. Efforts have been ongoing over the past several years by both NIST and NSA to develop and implement processes for evaluating and validating the security functionalities of both commercial and U.S. Government produced security and security enabled IT products. There continues to be a misconception that these processes result in the generation of a list of products that, when acquired and installed, provide guaranteed security for the systems in which they are used. Nothing could be further from the truth. There are no perfect security solutions and no particular product in and of itself will provide risk free security. Buyers and users of security products must understand that IA is more than just buying the right product. Rather, it must be a managed process which includes the acquisition of evaluated and validated products; risk management considerations which factor in the sophistication of the threat; an analysis of the system(s) in which the products will be used; proper installation, integration and testing of acquired products; and post-installation system certification and accreditation procedures. Additionally, trained and disciplined system administrators and network managers are critical to success. Finally, system configuration changes must be carefully managed and documented to assure continued security.